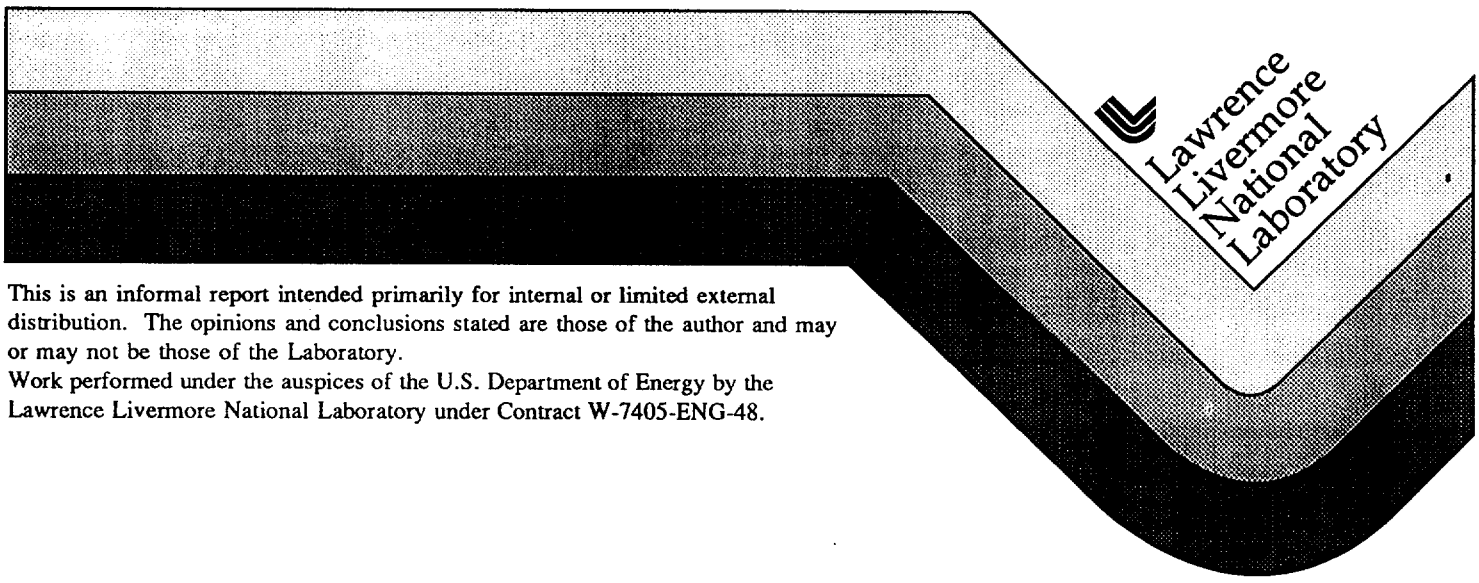
UCRL-ID-125763

Requirements for a Need-to-Know (NTK) Architecture

Nuclear Weapons Information Group
Computer Security Working Group

May 17, 1996



Work performed under the auspices of the U.S. Department of Energy by the Lawrence Livermore National Laboratory under Contract W-7405-ENG-48.

5/17/96
Version 1.0

Requirements for a Need-to-Know (NTK) Architecture

Nuclear Weapons Information Group
Computer Security Working Group

The purpose of this document is to present the requirements for a network architecture which can be used between sites within the DOE complex to transfer classified and sensitive unclassified information requiring need-to-know (NTK) separation. The network will not be a multilevel security system (i.e. support people with different clearances). All users will have a Q clearance. The architecture includes the hardware and software of the network components and computer resources connected to the network, the computer security features implemented, and the operational procedures needed to implement the network.

The approach we have used to develop these requirements has been to first identify the type of networking functionality which will be required between sites in order to accommodate major DOE initiatives, including weapons data archiving, ASCI, ADaPT, ES, and AMNII. These functional capabilities were called scenarios. The scenarios were written in a generic form in order to be used as test cases by the network implementers. The order of the scenarios in this document reflects the order in which the members of the Computer Security Working Group felt that they should be implemented. We added to each scenario the additional functionality required to insure that need-to-know control of the information is preserved. These additional functions are called the need-to-know requirements. As a result of this process we were able to identify those NTK requirements which are common among the scenarios and generalize in several areas: authorization, authentication, secure delivery, database access controls, and NTK monitoring.

We recognized that the network architecture will be implemented in phases because not all of the NTK requirements can be readily implemented. Some of the NTK requirements will be much more difficult to implement and may require investigation of new technologies or changes to existing network structures and operational procedures. (Those requirements which we think can not be easily met are marked with a pound sign.) The order in which the NTK requirements can be implemented depends somewhat on the cost versus benefit of solutions proposed. It is expected that management will not allow users to exchange classified information requiring need-to-know

separation until management is assured that sufficient mechanisms assuring NTK separation have been implemented.

We developed the requirements for the NTK architecture using the following assumptions. 1) A remote site is defined to be any group of people outside the user's organization. Therefore, within a site it is possible that a remote site might be simply a different functional organization (such as engineering); 2) The NTK architecture includes only networks and computer systems which have computer security plans already accredited by DOE and will include auditing and monitoring. We recognize that some aspects of the need-to-know separation have already been addressed in existing DOE orders and have tried not to reproduce them; 3) The NTK requirements presented in this document are the initial requirements and do not include any requirements for communications with the DOD or the UK. We recognize that some sites need to communicate with non-DOE organizations, but in the interest of getting a network implemented, the specification of such requirements will be done later; 4) These NTK requirements also do not include requirements for special access programs (SAP); Each SAP will have to be handled as a special case; and 5) The NTK architecture specified will apply to both classified and sensitive, unclassified information. Any differences between the requirements for classified and sensitive, unclassified information will be noted.

Need-to-Know (NTK) Scenarios

The NTK scenarios described below are arranged in order of usefulness as perceived by the committee members. It is recognized that some of the scenarios will be difficult to implement given the state of computer security and technology and may be implemented later. Such scenarios are considered long range goals and have been marked with a pound sign (#).

1 A user wants to exchange classified files (e.g. engineering drawings) with a user at a remote site.

2 A user wants to get classified information (e.g. drawings, database records) from a remote electronic repository (e.g. any server which stores classified information or indexes about classified information).

3 A user wants to use a classified computing environment on a remote computer from his desktop to run codes (including codes which transparently run or communicate with processes on other remote machines), debug codes, and create remote and local output.

4 A user wants to exchange classified email with enclosures with users at remote sites.

#5 A user wants to conduct classified video teleconferencing from his desktop to the desktop of a user at a remote site.

#6 A user wants to conduct classified interactive collaboration from his desktop to the desktop of a user at a remote site (e.g. video, audio and white board capabilities).

Need-to-Know (NTK) Requirements

The NTK requirements for the NTK architecture can be organized into several areas: authorization, authentication, secure delivery, database access controls, and NTK monitoring. The NTK requirements for each of these areas are described in this section. It is recognized that some of the requirements will be difficult to implement given the state of computer security and technology and that all the requirements will have to be met before the network will be fully functional. However, those requirements which are long range and will not prevent limited operation of the network have been marked with a pound sign (#).

1 Authorization

1.1 The NTK architecture must insure that users or machines which communicate with users or machines at remote sites have credentials which allow such communications.

1.1.1 Each user and machine which transfers or receives classified information (e.g. drawings, files, email and database contents) must be formally assigned credentials by site management based on an agreed-upon standard set of NTK criteria which specify the NTK groups in which the user or machine may participate.

#1.2 The NTK architecture must insure that a remote user or machine can only read or write the resources (e.g. disks and display screens) authorized by the user who owns the resources.

2 Authentication

2.1 The NTK architecture must insure that each user or machine which participates in a communication is actually the person or machine claimed.

2.1.1 Each site must insure that the identification (e.g. name and address) used to reach each user or machine is correct at all times.

3 Secure Delivery

3.1 The NTK architecture must provide the user with the option to request proof that the file or email received was the file sent by the claimed sender.

3.2 The NTK architecture must provide the user with the option to request that a delivery receipt be sent to him for the transfer of a file or email.

3.2.1 The receipt must include an indication of failure to deliver the information.

3.3 The NTK architecture must provide the user with the option to request that a formal record of the transmission of the file or email be created.

#3.4 The NTK architecture must insure that only the intended user or machine of the classified information or members of the same NTK group as the user or machine can access in an intelligible form the information transferred at any point during transit across the network.

#3.5 The NTK architecture must insure that a user or machine cannot get information from another machine for which the user or machine does not have an authorized NTK.

#3.6 The NTK architecture must provide mechanisms to limit the risks associated with exposing information stored on a machine to the system administrators of that machine.

#3.6.1 The NTK architecture must provide at least the capability to review the work of the systems administrators.

4 Database Access Controls

4.1 The NTK architecture must insure that a user or a machine serving as a proxy for a user which requests access to a database has proper credentials for the information to be accessed, including indexes and actual data.

4.1.1 Owners of databases must categorize or separate their data into identifiable "chunks" using an agreed-upon standard which can be used by the database server in conjunction with the user's credentials to determine what information is available to the user.

4.2 The NTK architecture must provide the capability to keep a record of which databases were accessed by a user or machine.

5 NTK Monitoring

5.1 The NTK architecture must provide the capability to determine if a user has been granted NTK capabilities which permit access to information which was not intended.

#5.1.1 The NTK architecture must provide at least the capability to detect if a user's access pattern represents a significant change in the amount of data or the number of databases accessed